IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHRISTOPHER SOGHOIAN (*pro se*)
1725 Irving St NW
Washington DC 20010
Ph: 617-308-6368
Email: chris@soghoian.net
Plaintiff,

v.

DEPARTMENT OF JUSTICE
950 Pennsylvania Ave, N.W.
Washington DC 20530,
Defendant.

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 522. Plaintiff Christopher Soghoian seeks injunctive and other appropriate relief for the processing and release of agency records related to various surveillance practices requested by plaintiff from defendant Department of Justice ("DOJ").

Jurisdiction and Venue

2. This court has both subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. §§ 552(a)(4)(B). This court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331. Venue lies in this district under 5 U.S.C. § 552(a)(4)(B).

Parties

3. Plaintiff Christopher Soghoian is a Washington, DC based Graduate Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Ph.D. Candidate at the School of Informatics and Computing at Indiana University. This complaint is filed in plaintiff's personal capacity.

4. Plaintiff's academic research is focused on the relationship between law enforcement agencies and communications companies, such as Internet service providers and telephone carriers. In addition to his role as an academic researcher, plaintiff is also a member of the media and self-publishes original, investigative journalism at his blog, Slight Paranoia (http://paranoia.dubfire.net). Plaintiff's research and investigative reporting is widely cited in the media, by academics and industry experts, and was also cited last year by Judge Kozinski in his dissent in *US v. Pineda-Moreno*, 617 F. 3d 1120, 1125, Court of Appeals, 9th Circuit 2010.

5. Defendant DOJ is a Department of the Executive Branch of the United States Government. DOJ is an "agency" within the meaning of 5 U.S.C. § 552(f). The Criminal Division and Executive Office of US Attorneys are components of defendant DOJ.

Plaintiff's FOIA Request and DOJ's Withholding Decision

6. By letter sent by fax to defendant DOJ's component Criminal Division on April 14, 2010, plaintiff requested under FOIA records concerning certain surveillance practices created between January 1, 2007 and April 13, 2010. Specifically, plaintiff requested:

    a. Any memos, email communications, reports, legal opinions, or other documents related to the government's acquisition (either compelled, or voluntary disclosure by the

carrier) of cellular location information (including but not limited to Call Detail Records) regarding individuals who are roaming, and thus not using their own carrier's network, and are instead using another wireless telecommunications carrier to which the individual is not a subscriber.

b. Any memos, email communications, reports, legal opinions, or other documents related to government requests for location of called parties in "hybrid" orders – e.g. requests that a carrier provide the government with subscriber and toll records for each number called by the target including cell site or location information associated with each call for a particular period.

c. Any memos, email communications, reports, legal opinions, or other documents related to government agents requesting and obtaining non-content header information (such as "to" and "from" addresses) associated with individuals' email communications that have been opened, or are over 180 days old, based upon a showing of relevance to an ongoing investigation (and not via a 18 USC 2703(d) order). Plaintiff also requested any information regarding refusals by some Internet Service Providers to deliver such non-content header information without a 2703(d) order, even for communications over 180 days old, and any information regarding DOJ's response to the refusal by the ISPs.

7. By letter to plaintiff dated February 11, 2011, the Executive Office of United States Attorneys ("Executive Offices") of DOJ notified plaintiff it had located four hundred and seventeen (417) pages of responsive documents, and that all 417 pages were withheld in full, pursuant to FOIA exemptions (b)(2),(b)(3), (b)(5), (b)(7)(C), (b)(7)(E), § 552a (j)(2), 18 U.S.C. § 2705 (b), § 3123(d) and § 3103(b). The Executive Offices advised plaintiff of his right to file an administrative appeal of the Executive Offices' adverse determination.

8. By letter to plaintiff dated March 28, 2011, the Criminal Division of DOJ notified plaintiff that it "located one hundred and eighty-six (186) records within the scope of [plaintiff's] request," and that all 186 pages were withheld in full, pursuant to FOIA exemptions (2), (5), (6), (7)(C) and (7)(E). The Criminal Division also notified plaintiff that it found "approximately four hundred eighteen (418) pages which originated by the Office of an United States Attorney. Pursuant to Department practices, [the Criminal Division] referred these pages to the Executive Office for United States Attorneys (which processes such pages) for its review and direct response to [plaintiff]." Finally, the Criminal Division advised plaintiff of his right to file an administrative appeal of the Criminal Division's adverse determination.
9. By letter sent by email to defendant DOJ's Office of Information Policy ("OIP") dated April 12, 2011, plaintiff appealed the Executive Office's determination to withhold requested records.
10. By letter sent by email to OIP dated April 16, 2011, plaintiff appealed the Criminal Division's determination to withhold requested records.
11. By letter sent to plaintiff dated April 25, 2011, OIP acknowledged its receipt of plaintiff's Executive Office administrative appeal received by OIP on April 12, 2011.
12. By letter sent to plaintiff dated April 28, 2011, OIP acknowledged its receipt of plaintiff's Criminal Division administrative appeal received by OIP on April 16, 2011.
13. To date, defendant DOJ has not issued a determination in response to plaintiff's administrative appeal under the FOIA.
14. Defendant DOJ has violated the applicable statutory time limit for rendering decisions on administrative appeals under the FOIA.
15. Plaintiff has exhausted the applicable administrative remedies.
16. Defendant DOJ has wrongfully withheld the requested records from plaintiff.

Background Information on Surveillance Practices

Surveillance of Roaming Users

17. The Stored Communications Act (specifically, 18 U.S.C. § 2703) regulates law enforcement access to the contents of communications, records concerning communications and other subscriber records. The statute only regulates government access to records about a "customer" or "subscriber." Plaintiff is interested in the extent to which law enforcement agencies can obtain records about wireless telephone or mobile device subscribers who are roaming on another carrier's network, and thus do not have a direct subscriber or customer relationship with that carrier.

Surveillance of Persons Within a Target's "Community of Interest"

18. In the late 1990s, researchers at AT&T created the Hancock programming language to enable efficient data mining of the company's telephone and internet access records. The system was originally created to develop marketing leads and as a security tool to see if new customers called the same numbers as previously cut-off fraudsters—something the original researchers referred to as "guilt by association."[1]

19. In 2007, it was revealed that Federal Bureau of Investigation (FBI) had been seeking "community of interest" or "calling circle" records from several telecommunications providers via National

[1] *See* Corinna Cortes et al., *Communities of Interest*, 2189 PROCEEDINGS OF THE 4TH INT'L CONF. ON ADVANCES IN INTELLIGENT DATA ANALYSIS 105, 110–11 (2001) (describing the tendency of 'fraudsters' to have closer links to other 'fraudsters' than a random account would have).

Security Letters, grand jury subpoenas, exigent letters, and email requests.[2] These records might include an analysis of which people the targets called most frequently, how long they generally talked and at what times of day, sudden fluctuations in activity, geographic regions that were called, and other data.[3]

20. A subsequent investigation by the Inspector General of the Department of Justice (DOJ) found that these powers had been widely abused by the FBI.[4] According to the Inspector General report, "[AT&T] records show that from 2004 to 2007, [AT&T] analysts [embedded within the FBI's Telecommunications Data Collection Center] used [AT&T's] community of interest [redacted] to review records in its database for 10,070 [redacted] telephone numbers."[5]

21. In May 2010, Albert Gidari, an attorney that represents several major wireless carriers, testified before the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties.[6] In advocating for reform of the Electronic Communications Privacy Act, Mr. Gidari described the "common" use of compelled requests for geo-location information associated with a surveillance target's community of interest:

---

[2] *See* Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES, Sept. 9, 2007, *available at* http://www.nytimes.com/2007/09/09/washington/09fbi.html.

[3] *Id.*

[4] *See* OFF. OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS (2010).

[5] *Id.*

[6] *See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29 (2010) (statement of Albert Gidari, Partner, Perkins Cole LLP).

"Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? It is common in hybrid orders[7] for the government to seek the location of the community of interest – that is, the location of persons with whom the target communicates."

22. Although these community of interest geo-location requests are "common," there is little public data available detailing the scale of their use, or for that matter, the number of requests for geo-location data regarding individual surveillance targets. Mr. Gidari previously revealed that requests to wireless carriers for customer location data have increased "exponentially" over the past few years, with major wireless carriers now receiving thousands of requests per month.[8]

[7] Law enforcement agents use "hybrid" orders to obtain cellular location information. Hybrid orders seek to determine a suspect's location based on non-content data transmitted by the suspect's cellular phone. The government has engaged in this type of surveillance by invoking a combination of authorities under the Pen Register Act and the Stored Communications Act. *See In re United States for Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435, 443-49 (S.D.N.Y. 2005); *See also In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (denying government request under "hybrid theory"), available at http://www.txs.uscourts.gov/district/judges/sws/05MJ557_Cell_site_opinion.pdf.

[8] *See* Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, February 19, 2010, available at http://www.newsweek.com/2010/02/18/ the-snitch-in-your-pocket.html.

Surveillance of "To" and "From" Non-Content Records

23. 18 U.S.C. § 2703(a) specifies that the government can use either a subpoena or an order issued under 2703(d) to obtain the contents of email communications that are older than 180 days.[9] Non-content information, however, can only be obtained pursuant to either a search warrant or an order issued under § 2703(d).[10] Email headers have long been considered to be non-content (although this does not include the subject line), which the Ninth Circuit confirmed in *United States v. Forrester*.[11]

---

[9] 18 U.S.C. § 2703(a) (2006).

[10] 18 U.S.C. § 2703(c) specifies that "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (*not including the contents of communications*) only when the governmental entity – obtains a warrant . . . [a 2703(d) order, or], has the consent of the subscriber or customer to such disclosure." 18 U.S.C. § 2703(c) (2006) (emphasis added). A few specific categories of customer records can be obtained with a subpoena. Pursuant to 18 U.S.C. § 2703(c)(2)(a) – (f), these are, "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)." 18 U.S.C. § 2703(c)(2)(a)–(f) (2006).

[11] *United States v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008) ("[E]-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed.").

24. Based on discussions with industry insiders,[12] it is plaintiff's understanding that Yahoo!, Google, and Microsoft have all established policies of scrubbing the "to" and "from" headers from email messages delivered to law enforcement agents in response to a subpoena. In such instances, if government officials wish to compel the disclosure of the headers from these three companies, they must first obtain a § 2703(d) order or search warrant. By taking this position, these companies have been able to force some degree of judicial review over a process that would otherwise bypass the courts.

25. Plaintiff has also been told that although DOJ does not favor the interpretation of ECPA adopted by these companies, it has not gone to court to compel the delivery of these headers pursuant to a subpoena.

CAUSE OF ACTION

Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records

26. Plaintiff repeats and realleges paragraphs 1-16.

27. Defendant DOJ has wrongfully withheld agency records requested by plaintiff by determining to withhold the requested material, and failing to comply with the statutory time limit for rendering decisions on administrative appeals under FOIA.

28. Plaintiff has exhausted the applicable administrative remedies with respect to defendant DOJ's wrongful withholding of the requested records.

---

[12] See Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, Minnesota Journal of Law, Science & Technology. 2011;12(1):191-237, 218, available at http://mjlst.umn.edu/uploads/62/2e/622e301ca428f23fbf40a98636e3334a/121_soghoian.pdf

29. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Requested Relief

WHEREFORE, plaintiff prays that this Court:

A. order defendant DOJ to disclose the requested records in their entirety and make copies available to plaintiff;

B. provide for expeditious proceedings in this action;

C. award plaintiff costs incurred in this action; and

D. grant such other relief as the Court may deem just and proper.

Respectfully submitted,

CHRISTOPHER SOGHOIAN
(*pro se*)
1725 Irving St NW
Washington, DC 20010
617-308-6368
Email: chris@soghoian.net